ISO 19600:2014 Compliance management systems - What does it mean for Europe?

Lillian Wylie
Compliance Manager, EAME & APAC
Oceaneering International Inc.

GLOBAL STANDARDS

• The United Nations Global Compact’s 10th principle against corruption, and the United Nations Convention against Corruption (UNCAC) – first globally agreed instrument against corruption which sets out a framework for action and implementation
• The OECD:
EUROPEAN STANDARDS

• Council of Europe Civil Law Convention on Corruption (1999)
• Council of Europe Criminal Law Convention on Corruption (1999)
• The European Union Convention on the Fight Against Corruption Involving Officials of the European Communities or Officials of Member States (1997)

AMERICA, AFRICA

AMERICA

• Organisation of American States Inter-American Convention Against Corruption (1996)

AFRICA

INTERNATIONAL CIVIL SOCIETY

• Transparency International’s Business Principles for Countering Bribery; and
• International Chamber of Commerce:

NATIONAL-LEVEL

• United States Sentencing Guidelines’ 7 Elements of an Effective Compliance Program;
• the US Department of Justice’s Resource Guide to the U.S. Foreign Corrupt Practices Act;
• the United Kingdom Bribery Act 2010;
• the UK Ministry of Justice’s Guidance on the United Kingdom Bribery Act.
SECTOR-WIDE INITIATIVES

• International Federation of Consulting Engineers Code of Ethics & Policy Statements
• International Council on Mining and Metals Sustainable Development Charter, Ten Principles
• UNICORN, Trade Union Anti-Corruption Network
• The Extractive Industry Transparency Initiative
• Healthcare compliance initiatives

ISO CONTRIBUTIONS

• A new ISO standard, ISO 37001, specifically targeted at anti-bribery compliance is currently in draft format, expected in Q3 2016.
• Key difference: ISO 19600 exhortatory guidelines, e.g. ‘should’. ISO 37001 sets out requirements, e.g. ‘shall’ & is therefore certifiable.
What does ISO 19600 cover?

ISO 19600 is structured into seven distinct parts:
• context of the organization;
• leadership;
• planning;
• support;
• operation;
• performance evaluation;
• improvement.

Recognisable Approach

The standard has followed a recognizable method of:
• commitment,
• design,
• implementation and
• continuous improvement.
Leadership

US Sentencing Guidelines (USSG):
1) Leaders understand and oversee the compliance program to verify its effectiveness.
2) Specific individuals have the authority and responsibility to carry out the program.
3) The company denies leadership positions to people who have engaged in misconduct.

OECD Guidelines for Multinational Enterprises:
1) Support from senior management is strong, explicit and visible.
2) Program is overseen by senior corporate officers with sufficient resources, authority and access to the board.

UK’s Guidance 6 Principles:
Principle 1 - Top-level commitment.

ISO: Leadership, including:
1) the establishment and championing of a strong value-driven culture for the company;
2) commitment (both words and action) from the senior management team to the goals of the compliance program;
3) commitment of appropriate resources;
4) a clear, comprehensive compliance policy endorsed by the executive; and
5) a clear outline and assignment of organizational roles, responsibilities and authorities (e.g. for the governing body/top management, the compliance function, management and employee).

Risk Assessment

USSG:
Companies must conduct periodic assessments of risk of criminal conduct and take appropriate steps to design, implement or modify each element to reduce risk.

OECD:
Risk assessment should be the basis for effective internal controls and compliance programs.

UK’s 6 Principles:
Principle 2 - Broad categories of risk must be carefully examined, including country, sectoral, transaction, business opportunity and partnerships.

Principle 3 - Program priorities, resources and controls should be determined based on the results of the risk assessment.

ISO:
Understanding the organization at hand, and its context, needs and requirements.
Standards & Controls

USSG:
Companies should have standards and procedures to prevent and detect criminal conduct. They should provide incentives and discipline misconduct.

OECD:
1) Company policy should clearly and visibly state that bribery is prohibited.
2) Compliance programs should address key risk areas.
3) Companies should conduct due diligence on business partners and implement effective internal controls for accurate books and records.
4) Employees should be able to report violations confidentially without fear of retaliation.

UK’s 6 Principles:
Principle 4
1) Policies and procedures should be clear, practical and accessible.
2) Companies should have due diligence protocols for screening third-party intermediaries.

ISO:
Planning:
1) Compliance objectives should be consistent with the compliance policy, measurable, practicable, monitored, communicated and updated as appropriate; 
2) the organization should clearly determine how to achieve these objectives, including resources required, responsibility and target completion dates; 
3) these efforts should be documented.

Training

USSG:
1) Companies must communicate the standards and procedures of its compliance program and conduct effective training.

OECD:
1) Training should be periodic, consistent, and documented.

UK’s 6 Principles:
Principle 5 - Effective implementation of compliance program policies and procedures through adequate training.

ISO:
1) Support necessary to implement a compliance management system, including:
1) adequate resources (including access to organisational infrastructure, finance and human resources, external advice and contemporary reference material on best practice compliance and legal developments);
2) competence and training (including maintaining records);
3) organizational awareness of the compliance program, the role an individual plays in contributing to and maintaining the program, and the implications of not conforming with the compliance management system requirements;
4) the development of a compliance culture via active, visible, consistent and sustained commitment of the governing body and management towards a common published standard of behaviour; and
5) the need for documented information regarding the operation of the compliance program.
Oversight

USSG:
1) Companies should monitor and audit their compliance programs and maintain reporting mechanisms.
2) They should respond quickly to allegations and modify their programs as needed.

OECD:
1) Individuals at all levels of the company should be responsible for monitoring.
2) Companies should discipline employees for violations of the policy.
3) Companies should regularly review their compliance programs and make necessary revisions.

UK’s 6 Principles:
Principle 6: Companies must monitor and review their compliance programs.

ISO:
Performance Evaluation:
1) monitoring, measurement, analysis and evaluation, including the development of measurable indicators to assist the organization in measuring the achievement of its compliance objectives (e.g. percentage of employees trained effectively);
2) auditing practices; and
3) management review.

Non-conformance & Continual Improvement:
1) in the event of nonconformity, noncompliance and corrective action; and
2) continual improvement.

Current Approach to Dealing with Multiple Standards

A hodge-podge mix of:

- the highest common denominator – e.g. ascertain the requirements of the most exacting standard applicable and apply these requirements;
- local law – recognising the local jurisdiction of operation and making reference to that law (however cursory) in the compliance program;
- law of the parent company (if different to the local law, as is often the case);
- the standard published by the CEO’s favourite industry association.
Questions for the profession

Q: What do we think about this situation?

Q: Are we happy with it?

Q: Would we prefer to change the status quo?

Q: Assuming we do want to change the status quo, what do we want the new landscape to look like?

A new status quo?

Key elements of a new status quo might include:

- Single source of truth, clearly acknowledged authoritative standard
- Impartial/non-partisan/global
- Authoritative
- Clear
- Principles-based
- Acknowledged by domestic authorities (e.g. local courts) as best practice
Advantages

• Central Authoritative Body
• Multinational Companies
• International Trade
• Investor/Customer Benefits

Disadvantages

• Costs of transition
• Vagueness of a principles-based approach
• Lack of individual tailoring to situation at hand
The way forward

• Do we want a continuing proliferation of guides?
• How should we attempt to rationalize it?
• What would be the most acceptable overarching global guide (if any)?

ISO

• “ISO is an independent, non-governmental international organization with a membership of 162 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.”
ISO KEY AREAS

• Health;
• Sustainable Development;
• Food;
• Water;
• Cars;
• Climate change;
• Energy efficiency and renewables;
• Services

• What are the implications for Europe?

• What are the implications of Europe for ISO?

• Where to from here?